(54) Title: A SYSTEM AND A METHOD RELATING TO USER PROFILE ACCESS CONTROL
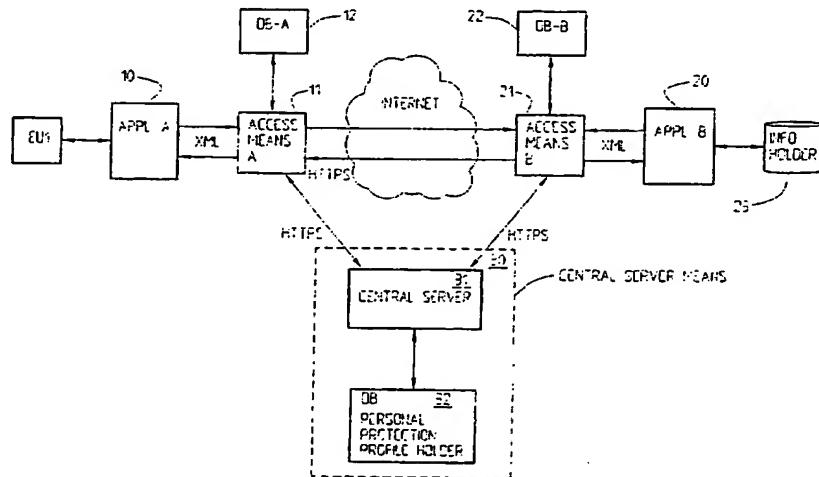
(57) Abstract: A system for end user control of the distribution and maintenance of end user personal profile data in a data communications system providing communication between applications comprising and/or communicating with service/information/content providers or holding means (DB) holding end user personal profile data. It comprises a personal profile protection network with at least one central protection server means, comprising or communicating with information holding means holding personal protection profile information, and a number of distributed access means, e.g. software modules. For each of said applications at least one access means is provided, and grant/reject of an access request for/to end user personal profile data by a requesting application is determined by the central protection server in communication with a requesting application and/or an information providing application. Translating means are provided for identity translation and the identity of a requesting application will be concealed for an information providing application, and vice versa.

A SYSTEM AND A METHOD RELATING TO USER PROFILE ACCESS CONTROL

5

FIELD OF THE INVENTION
The present invention relates to a system allowing end user control of the distribution and maintenance of end user personal profile data, i.e. data within personal profiles, in a data
10   communication system providing communication between applications, which comprise and/or communicate with service/information/content providers holding end user personal profile data. The invention also relates to a method of controlling access to personal profile data within a personal end user profile in a data communication
15   system running a number of applications, comprising or communicating with information/content/service providers. The data communication system may be third party controlled, or alternatively it is not.

20   The invention also relates to a personal profile data control network for controlling the access to personal profile data.

STATE OF THE ART
In the information society of today the personal profile data of
25   end users will be more and more spread out at different locations e.g. on Internet, and with the fast development of global data communication networks, it gets possible to distribute data both via fixed and via wireless applications. Data will also be pushed out to an even higher extent than hitherto, e.g. by companies to
30   other companies etc. The need for means to protect privacy therefore increases. For the individual end user it is exceedingly important that his personal information can be protected from uncontrolled distribution among end users, companies etc. At the

2

same time as, for example, the number of services that can be provided to end users, over for example Internet, increases, it becomes more and more interesting for service and information providers to be able to obtain detailed information about users.
5   This may be in conflict with the privacy aspect for the end users, as well as it of course also may be attractive for the end users, since they can also take advantage of personal information being spread out, and thereby obtain other useful or desired information etc. For statistical purposes it is interesting for e.g. companies
10   to get information in order to become familiar with the needs for services, products etc. An end user may today have stored personal profile data of different kinds, at different locations, which contains various kinds of information about the user, such as name, address, particulars habits, hobbies, accounts, financial
15   situation etc. Thus, it is exceedingly important for the service/content providers to know the characteristics of existing and potential customers to allow for targeted advertising etc., at the same time as it is also exceedingly important for the end user to be able to protect the personal profile data.
20

Thus there is an inherent conflict between different interests. Therefore laws and regulations have been created in an increasing number of countries, such as for example within the European Union, to restrict the accessibility to privacy information. Such
25   laws and regulations often vary from one country to another, but generally they have in common that the consumer or the end user should have control over his or her profile, including conditions for its release.

30   Solutions have been suggested for systems for protecting user personal profile data acting as a kind of a safe or functioning as a profile repository. The profiles can, by replacement of the user identity, for example the mobile phone number, through a code, be

stored such that there will be no connection to the user identity, throughout the network. Such a repository or storing means for user profiles can be arranged at different nodes within the network. One example is illustrated in Fig. 1, with a profile holding means provided between a portal and an advertising node. In Fig. 1 it is supposed that the personal profile has been transferred to the advertising node, with the user identity in the form of a mobile phone number (MSISDN or MIN) replaced by a code, which is totally unrelated to the phone number. The procedure will then be that the portal requests an advertisement for a user, e.g. with a phone number, 1. The profile holding means then forwards the request to the advertising node with the mobile phone number converted to a corresponding code, 2. The advertising node subsequently returns the advertisement to the personal profile holding means, 3, which subsequently returns the advertisement to the portal, 4. Such a system is for example known under the trademark Respect ™ which is an e-business platform enabling privacy control, identity management and instant personalization for on-line transactions. The profile holding means is then represented by the Respect ™ server which is a virtual infrastructure located at the mobile Internet provider.

However, there are several problems associated with systems as described above. One main issue is the transactional capacity of the profile protecting means. Normally the number of users that can be handled is limited, which results in serious problems for real time applications. With reference to the example given above, advertisements have to be served when an end user actually visits a particular page, or accesses a particular service, and many operations are time-critical. The time criticality is particularly important in wireless environments.

4

Another problem relates to the lack of generality when handling flows from several requesting nodes and from several information holding nodes. Another problem that is not solved in a general manner is really pertinent, and it is concerned with which nodes

5   that should be allowed to request data from other nodes. Mapping between a code, for example known by the advertising node, and the phone number, as known by the portal, is actually performed in the profile holding means, also called a profile repository. It is not acceptable that for example the requesting portal asks the profile

10   repository for the corresponding code, and then requests an advertisement for this code since, then the phone number and the code would be visible together.

SUMMARY OF THE INVENTION

15   In order to solve these and other problems a system is needed through which end users are given the possibility of controlling which information, within a personal profile, that should be accessible by others, for example via applications etc, i.e. to be able to protect their private information at the same time as

20   being given the opportunity/ possibility of taking advantage of allowing access to others in order to get information etc. that is of interest for the specific end users, in a substantially automatic manner, and without expressively having to request such information.

25

It is also an object of the invention to provide a system which makes it possible to interconnect a large number of different information applications and service enablers or service/content/information providers while maintaining privacy

30   and dynamical information routing. It is also an object to provide a system through which applications can be connected to the appropriate information/service/content providers or information holders without these applications having to know the address of

5

the actual information holder or information provider. It is also an object to provide a system to facilitate for applications to find the information that is desired within the network, while still duly considering privacy requirements and restrictions.
5   Further yet it is an object to make connection to applications as simple as possible, and without requiring different interface solutions for different kinds of providers, end users etc. It is also an object to find a solution allowing for locking/unlocking of private or personal information, particularly in a fast and
10 easy manner, and in addition thereto to provide for a highly scalable system, as far as protection of data within personal profiles is concerned.

Still further it is an object to provide for easy and flexible
15 control of private or personal information within fixed as well as within mobile data communication networks, such as for example Internet, Mobile Internet or private IP based Wide Area Networks (WAN), and to allow for a high scalability as far as equipment and networks are concerned, and also to support load sharing and
20 redundancy solutions on network level.

A main object of the invention is to allow for anonymous IP addressing and anonymous provisioning of information. Still other objects are concerned with the provisioning of easy operation and
25 maintenance, while still allowing for a privacy protection facility, and to reduce management requirements as much as possible, as far as privacy protection is concerned. It is also an object to suggest a solution that allows for, optimizes and facilitates, protection of personal information both as far as the
30 end user is concerned, and as far as the operator and application provider are concerned. Particularly a solution is needed through which also problems associated with the use of discontinuous protocols or Application Programming Interfaces (API), such as for

example HTTP (Hypertext Transfer Protocol) as opposed to for example E-mail services using continuous protocols like SMTP (Simple Mail Transfer Protocol), are concerned.

5   Moreover it is an object of the invention to provide a solution which both makes it easy for the end user to control the flow of personal information, e.g. between different companies, as well as makes it possible for for example companies or application providers handling personal, private information, to meet the
10   requirements of laws and regulations for respecting privacy, and at the same time to be able to provide services based on personal information, for example position data. It is also an object to enable for example for an application provider to directly, in a digital way, get permission by the end user (indirectly), to use
15   the requested information.

A personal profile data control network and a method respectively, of controlling access to personal data within personal end user profiles, are also needed, through which one or more of the above
20   mentioned objects can be fulfilled.

Therefore a system as initially referred to is provided, which comprises a personal profile data protection network with at least one central protection server means, comprising or communicating
25   with information holding means, e.g. a database, holding personal protection profile information, and a number of distributed access means, for example comprising software modules. For each one of said applications at least one access means is provided, and grant/reject of a request for access to end user personal profile
30   data within a profile by a requesting application is determined by the central protection server in communication with the requesting application and/or the information providing application, or more specifically in communication with the corresponding access means

thereof. Translating means, e.g. comprising encrypting means, are provided for identity translation and verification, and the identity of a requesting application will be concealed for an information providing application and vice versa. This means for example, that an application provider does not know where a requested piece of information is located and the operator of such a personal profile data control network or privacy information network, does not have to expose the addresses between application provider or information provider and requester. Particularly there is one access means for each application. Alternatively there may be a plurality or a cluster of access means for at least one application or for all applications, e.g. for redundancy reasons and/or to allow for load sharing at the site of the application. The server means at a site, particularly the protection profile holding means associated therewith, may also be redundant. Redundant server means (servers and/or profile holding means) may be provided; at a site or distributed.

Particularly the central server means only comprises personal protection profile data. This means that it does not contain any personal profile data as such, which is distributed throughout the system. The personal protection profile data comprises information about, for each end user of the system, which personal data within the end users personal profiles that should be accessible by which application, and/or vice versa, which data should not be accessible etc. In one implementation the personal protection profiles are assigned one of a given number of security levels, the lowest level e.g. indicating that all personal profile data should be inaccessible to every application, the highest level for example indicating that all personal profile data should be freely available, particularly with due regard to applicable laws and regulations. Of course a number of alternative ways of indicating which data should be accessible by whom etc. are possible, the

8

main thing being that it is end user controlled and easily
settable and update-able by the end user himself, so that end user
in an uncomplicated manner is able to control who should get
access to which personal data.

5

Particularly each application and the respective, thereto
belonging, access means are interconnected over an interface, an
Application Programmable Interface (API) based on a generic markup
language. In a most advantageous implementation the generic markup
10   language is XML (Extensible Markup Language).

In a preferred implementation access to requested end user
personal profile data, i.e. data within an end user personal
profile, is granted/rejected by the central server in
15   communication with the requesting application. In an alternative
implementation access to requested end user personal profile data
is granted/rejected by the central server means in communication
with the information providing application. In still another
implementation, e.g. in case the access means of the requesting
20   application cannot be trusted, access to requested data may be
granted/rejected by the central server means in communication with
both the requesting application and the information providing
application. This, however, is somewhat inefficient in that
additional encryption/decryption steps are required, as well as
25   additional transmissions are necessitated. In a particular
implementation (first) user identity translating or encrypting
means are provided at least in the central server means. Further
(second) identity translating means may alternatively also be
provided in the access means of the requesting application and/or
30   the information providing application. A first validation of the
request may, according to the most preferred embodiment, wherein
only the access means of the requesting application is in
communication with the central server means, be carried out in the

9

access means of the requesting application. However, a further validation is also performed in the access means of the information providing application relating to its communication with a database holding the information being the object of the access request.

According to the invention particularly each service offered by the system to information-requesting applications is assigned a unique DTD (Document Type Definition). The DTD can be said to consist of rules controlling the communication between e.g. a requesting side and a providing side by defining which data that is allowed to be transferred between the two parts or sides, and the associated data to be transferred.

Each information-providing application will agree with the central server means on a "general DTD". This embodies the maximum number of data fields the information-providing party will release. Specific end users may, by interacting with the central server means, create user-specific DTDs and thereby reduce the data allowed to be released pertaining to their IDs. Furthermore, the central server means offers "general DTDs" to information-requesting applications to describe what a particular service offers, prior to any end user-specified reductions of data to be released.

In a most preferred implementation a request for access to end user profile data is transported from the requesting application to its access means using RMI (Remote Method Invocation) whereby the request is transported as an XML transport object (in an XML node tree container) tagged with information about the requested end user personal profile data. Information between an access means and an application can alternatively be sent e.g. as an XML string. Instead of RMI may e.g. CORBA™ or SOAP be used. For

10

communication between the access means of the requesting/information providing application respectively, and the central server means, is particularly the HTTPS protocol (Hypertext Transfer Protocol Secure) used. XML SOAP, CORBA™ etc.

5   may alternatively be used.

In a preferred implementation the request is digitally signed by the access means of the requesting application (with a private key of the access means) and/or by the access means (a private key thereof) of the information providing application. Preferably it

10   is also signed by the central server means using a private key thereof. In a most preferred implementation the request, when having been communicated to the central server, which responds with an end user-specific DTD, is validated by the access means of

15   the information-providing application. In an alternative implementation it is validated by the access means of the information requesting application. (The preferred place to validate a request depends on business circumstances. For example, if information-providing applications require payments for

20   communicating with their access means, information-requesting applications might prefer to validate the request prior to communicating with the information-providing party. Furthermore, a reason for emphasizing validation in the information-providing application's access means is the eliminated risk of unauthorized

25   release of data due to a "hacked" access means belonging to the information-requesting application.)

Digital signing at an access means (and in the central server means) may be optional, e.g. if the security is considered to be

30   sufficient since the communication or exchange of information takes place within a network controlled by one and the same operator, or if the data need not be protected. Digital signing procedures are controlled by the central server means, and to

which extent digital signing is to be implemented, and where, is thus end user controlled.

Particularly the central server means encrypts the user identity
5   for the requested information used by the information providing application. In addition, or alternatively, in other, preferred, implementations, encryption of the user id used by the requesting application is performed.

10 In an advantageous implementation the system includes a cache memory associated with each application respectively, for temporarily holding information about access requests, such that a previously used session can be reused, at least for a given time period. It should be clear that each access means is associated
15 with a database or similar, particularly a proprietary database holding ·for example general DTD information and address information. The information providing application generally does not hold the information but fetches it from an information holder, e.g. a service/content/information provider or a database.
20

To solve one or more of the problems initially referred to the invention also suggests a personal profile data access control network for controlling the access to personal profile data. The network comprises at least one central protection server means,
25 comprising or communicating with information holding means for holding personal protection profile information, and a number of distributed access means, e.g. software modules, at least one access means respectively interfacing each of a number of applications. The central protection server means comprises means
30 for translating and verifying identities. A request for access to personal profile data by a requesting application is communicated to the access means of the requesting application and it is granted/rejected by the central server means in communication with

the access means of the requesting application and/or the established information providing application. The identity of the requesting application is concealed from the information providing application and vice versa. The interface between an application and the respective access means is based on a generic markup language, which advantageously is XML. Particularly the, with the central server means, associated information holding means contains personal protection profiles for each end user registered with the system, and the personal protection files are end user controlled. Preferably the central server means and the access means of the requesting/information providing applications digitally sign the requests for personal profile data with their respective private keys, and the digital signatures are verified by the control logic of the central server means and the access means respectively using the respective corresponding public key.

The invention also suggests a method of controlling access to personal data within personal end user profiles in a data communication network, running a number of applications, and comprising or communicating with information/content/service providers. The inventive method includes the steps of; providing an access request from a requesting application to an access means associated with the requesting application using a generic mark-up language, e.g. XML; forwarding the request from said access means to a central server means with information holding means holding personal protection profiles for the end users of the system; performing user identification translations/encryptions such that the user identification of the requesting application will be concealed for the information providing application and vice versa; establishing, by using the request and the personal protection profile, whether access is to be granted or rejected; if access to the requested personal profile data is to be granted; confirming to the access means of the requesting application that

access is to be granted; validating the response to the request
sent to the central server means; transmitting the translated
(encrypted), preferably digitally signed, request to the access
means of the information providing application.

The request of a requesting application particularly relates to
getting access to data in (fetching data from or setting data in)
a personal profile, and, the method particularly further may
comprise the step of; using a third party controlled data
communication network, e.g. Internet or another IP-based network,
for communication between the requesting application and the
information providing application, particularly using e.g. the
HTTPS protocol.

Preferably the method includes the step of digitally signing the
request in the access means of the requesting application before
sending it to the central server means; performing an encryption
of the user identity used by the information providing application
in the central server means, signing the request in the central
server means; validating the response to the request in the access
means of the requested application; digitally signing the request
in the access means; decrypting the user identity used by the
information providing application in the access means of the
information providing application, and digitally signing the
request; transferring the request to the information providing
application; accessing the requested data and signing the response
in the information providing application; transmitting the
requested data, if applicable, to the access means of the
information providing application; digitally signing the requested
information; sending the access granted information to the access
means of the requesting application over the third party
controlled data communication network using e.g. HTTPS; digitally
signing the information message in the access means of the

14

requesting application; sending the requested information data to the requesting application (e.g. using RMI). If data is to be set in a personal profile, it is instead the response to the request that is returned to the requesting application.

5

BRIEF DESCRIPTION OF THE DRAWINGS
The invention will in the following be more thoroughly described, in a non-limiting manner, and with reference to the accompanying drawings, in which:

10

Fig. 1   is a schematical block diagram describing a state of the art system,

Fig. 2   very schematically illustrates the personal profile
15   data protection network in communication with applications, providers etc.,

Fig. 3   is an illustration of a system allowing end user protection of personal profile data according to the
20   invention,

Fig. 4   schematically illustrates a specific implementation of a system as in Fig. 3,

25   Fig. 5   schematically illustrates an alternative embodiment implementing a cache functionality,

Fig. 6   schematically illustrates a further alternative implementation of a system according to the invention,

30

Fig. 7   is a flow diagram describing one implementation of the concept when data within a personal profile is requested via a requesting application,

Fig. 8   is   a   simplified   flow   diagram   illustrating   an
             implementation with a cache, as described in Fig. 5,

5   Fig. 9   is   a   flow   diagram   illustrating   one   particular
             embodiment according to which the user identity should
             not be recognized by the requesting application,

Fig. 10   is   a   flow   diagram   describing   an   alternative
10   implementation when the user identity should not be
             recognized by the requesting application,

Fig. 11   is   a   flow   diagram   schematically   illustrating   the
             central server means updating the distributed access
15   means, and

Fig. 12   is a flow diagram describing end user setting of a
             personal protection profile in a central server means.

20   DETAILED DESCRIPTION OF THE INVENTION
     The state of the art solution as schematically indicated in Fig. 1
     has already been discussed earlier in the application under the
     section "State of the art" and will therefore not be further
     described herein.
25

     Fig. 2 is a schematical illustration of a personal profile
     protection network or privacy information network. According to
     the invention different information applications can be connected
     with several service/information/content providers including
30   privacy protection and dynamic information routing. Through the
     personal profile protection network applications, information
     providers, service providers, content providers and other privacy
     information networks are interconnected, making it possible to

16

connect in any appropriate manner requesting applications with
information providing applications or providers, without the
applications having to know the addresses of each other. Large
personal profile protection networks can be built on for example
5   Internet, Mobile Internet or any private IP based WAN (Wide Area
Network).

Fig. 3 shows one example of a system according to the invention.
The system includes an application A 10 with access means A 11 and
10 an application B 20 with access means B 21. Each access means 11,
21 communicates with a database, DBA 12 and DBB 22 respectively.
The access means 11, 21 form part of the personal profile data
protection network and communicate with a central server means 30
comprising a central server 31 and a database 32 holding personal
15 protection profile information.

The access means interfacing an application may comprise one
single, or two, or more access means, or even a cluster of access
means, for example depending on redundancy and load sharing
20 requirements on the application site.

The central server means handles or controls the information
routing and personal profile data locking/unlocking. Of course a
personal profile data control network may comprise more than one
25 central server means and a plurality of (singular or multiple)
access means, but for reasons of clarity only two access means,
one for each application, and one central server means are
illustrated in the figure. For redundancy there may also, or
alternatively, be more than one central server at a site, or at
30 multiple sites. There may also be at least duplicate information
holding means associated with a central server.

It is here supposed that application A 10 is the requesting application, here communicating with end user EU 1 and it may for example request access to personal profile data located anywhere in the network, either for the purpose of fetching the data, or
5   for the purpose of setting new data in the personal profile. Both getting and setting (pull and push) of data is covered by the inventive concept, and the functioning is in principle similar.

It is here further supposed that the application B 20 is an
10 information providing application that finds the data in information holding database 23.

In the databases 12,22 of the access means 11,21, information is contained about which is the central server that handles the DTDs
15 needed for the communication between information requesting and information providing applications, and the databases 12,22 do also contain the address, e.g. IP number based URL:s (Uniform Resource Locator) of the (appropriate) central server means.

20 The access means A 11 does not know where to send the request received from application A 10. Access means A 11 is interfaced with application A 10 over an XML object based API (Application Programming Interface). Preferably each application uses RMI (Remote Method Invocation) for communication with its respective
25 access means. For communication between an access means and the central server means e.g. HTTPS is used. Access means belonging to different applications also communicate using HTTPS e.g. over Internet or another IP based communication network.

30 This figure does not show in detail how the communication is carried out, but it illustrates a general system that can be used in different ways. In one implementation, however, (cf. also Fig. 4) application A 10 sends a request for personal profile data to

its access means 11 using XML objects or text. Access means 11
does not know what to do with the request and questions its
database DB A 12 to find out the address of the central server
means to which the request should be forwarded. Via HTTPS the
5   request is forwarded to the central server 31 which establishes,
using database 32 containing personal protection profiles whether
the access request should be allowed or not, i.e. whether the data
may be accessed or not by the particular requesting application.
An indication of a rejection or a grant of the access is returned
10   to access means A 11, which in case of grant, then uses HTTPS for
communication with access means B 21, which in turn validates the
request and, if the validation was successful, requests
application B 20 to access to the data, which in turn accesses the
data in information holder 23. Subsequently information is
15   returned to application A 10 via access means B 21 of application
B 20, over Internet to access means A 11. In access means B 21 may
optionally a manipulation or modification of returned data from
application B 20 be performed.

20   The communication with the central server means may alternatively
be performed exclusively via access means B 21. It should be clear
that each access means can be used in a similar manner
independently of whether the interfaced application acts as an
information requesting application or as an information providing
25   application.

The used XML object based API can easily be interfaced without
requiring protocol conversions, and it is based on information
level communication which does not expose the implementational
30   details between involved elements. Every new type of information
service that is needed only needs a new DTD for the information
that has to be transported, which provides a standard way to allow
for integration between information products, having as a result

19

that different applications do not have to implement new APIs for different types or formats of information to be transferred, instead the DTD is changed or replaced.

A fundamental characteristic of the system according to the invention is that access rights to personal information are administrated by the end user at a central location, i.e. at the central server means, whereas the personal profile data, i.e. the information as such, is distributed throughout the communication system or communication network on different sources. One reason therefore is that it is not really plausible to keep all personal information at one and the same location. Another reason is that personal data can be highly dynamic, an example thereon is the position of a user in a mobile network. Another example relates to the balances of user's check accounts which can also vary rapidly. It also facilitates for an end user to protect the personal data in an environment with a large number of information requesters and a large number of information providers, and therefore it has been found that it is extremely advantageous to provide the end user with a central facility where the end user can lock/unlock, i.e. customize access to, personal information from different providers and to different information requesters.

According to the invention an information requesting application does not know the identity of an information providing application or information holding means and vice versa. The only way to send personal profile data from an information holding side to an information requesting side is by translating the identities, preferably in the central server. This means that there will be no connection between personal information from different locations without going through the user controlled central server means. By having the personal profile data or information spread out at different locations, or at the same location but unrelated, with

different user identities, the result will be that mining of the
end user privacy is not possible. The central server means only
holds information about which personal data that is locked and
unlocked respectively, it does not "own" the actual information.

With reference to Fig. 4 an advantageous implementation will be
more thoroughly described. It is supposed that an information
requesting application 10_1 wants to pull (get) information from an
information providing application 20_1 without knowing where to
find the information itself. In this implementation it is supposed
that communication with the central server means is provided by
the access means 11_1 interfacing the requesting application 10_1.
The advantage of such an implementation is that a fast preliminary
response is obtained from the privacy network, i.e. from the
central server means 30_1, as to whether the requested transaction
is possible, without even having to involve the access means 21_1
of the information providing application 20_1 (or the information
providing application itself). The load resulting from rejected
transactions on the access means 21_1 on the information providing
side will thus be considerably reduced as compared to a case when
the providing side is involved at an early stage.

Thus, when the information requesting application 10_1 wants to set
information in, or get information from, an information provider,
or holder, the requesting application 10_1 makes a request towards
"its" access means 11_1. The requesting application does not know
the address to the information provider. It is further supposed
that access means 11_1 holds a public key and a private key. The
private key PKI (Private Key Infrastructure) of a node may e.g. be
stored as a key object, e.g. a secured object file.

In a particular implementation the request is sent over RMI, and
it preferably contains:

- the user identity (ID) associated with the request and used by the requesting application,
- a DTD ID (equivalent of a service ID),
5   - a Transaction ID,
- an ID of the Requesting Application,
- a Gateway ID, and
- an XML Node Tree Container.

10 The XML Node Tree Container contains an XML node tree tagged with which information the requesting application wants to get or in which personal data fields he wants to set data, update data etc. The tagged XML node tree may e.g. be described as a form, an XML node tree form.

15

The XML Node Tree Container is an object for transportation of the XML Node Tree between the requesting application and its access means 11_1. I indicates a request from the requesting application 10_1 to the access means 11_1. Access means 11_1 finds the general DTD

20 – i.e. a DTD not yet tailored to specific end user preferences on the transfer of personal data, the general XSLT file, the Public Key of the central server means, DNS (Domain Name Server) names and IP addresses (one or more IP number based URLs in order from the main central server means for the DTD ID, in case there are

25 more than one central server means).

In one implementation it may be an option to look up a specific central server means ID, if it is specified in the database (DB-A 12) with a specific central server means public key. This may be

30 used when the central server means is not one in the cluster with the same public key, but e.g. one which uses the same domain name. The relevant information for central server means ID, DTD

information etc. is fetched by the access means 11_1 from the associated database 12_1.

The access means 11_1 of the requesting application 10_1 then sends the request on, II, to the central server means 30_1 to find the specific DTD for this particular service and end user ID. Particularly HTTPS is used, and the request particularly comprises:

- the identity of the requesting application access means 11_1,
- the digital signature of the requesting application access means with its private key,
- the end user ID used by the requesting application 10_1,
- the DTD ID (equivalent of a service ID),
- the Transaction ID,
- the Gateway ID, and
- the requesting application ID.

A response is then awaited and expected from the central server means 30_1. In the meantime, while awaiting the response, the requesting application access means 11_1 optionally validates the XML node tree with the general DTD for the DTD ID (service ID). This constitutes a basic validation and it is done the first time the DTD ID is used, from the time that the server is up and running in order to limit the load on the requesting application access means 11_1.

The central server 31_1 comprising control logic, checks the authentication of the request with the identity of the access means, the IP address (optionally) and the digital signature against the public key of the access means 11_1. The requesting application user ID and the DTD ID are then mapped onto the information providing application user ID. It should be noted that

the user identity used by a requesting application can be, or normally is, different from the user identity used by an information providing application. Further, the user identification used by an application is not the identification of
5   the application.

The information providing application 20_1 user ID is encrypted with date/time using the public key of the access means 21_1 of the information providing application 20_1, such that it only can be
10 read and understood by the information providing application access means 21_1. The encrypted pattern should be different every time the access means 11_1 of the requesting application 10_1 makes a request. The central server 31_1 gets a digital signature for the end user specific DTD from the database holding protection profile
15 information 32_1, signed with the private key of the central server means 31_1. To obtain a good performance, DTDs may be signed in advance. "Out of band" information elements are also signed. (By "out of band" information is here meant the systems level communication layer, e.g. including control information for the
20 access means. This can e.g. be implemented as HTTP POST in the forward direction and as a cookie in the backward direction.)

The central server means 31_1 then, III, returns messages to the requesting application access means 11_1 containing the end user
25 specific DTD as in band information. (By "in band" is here meant information at the application data communication layer, e.g. at XML document level.) The central server means 31_1 also returns "out of band" information such as:

30 - the digital signature of the end user specific DTD,
    - the digital signature of the central server means "out of band" information,
    - the identity of the central server means,

24

- the encrypted end user ID, i.e. the information providing application end user ID,
- time to live,
- inactivity time,
5 - response time,
- the domain name of the access means 21_1 of the information providing application 20_1,
- its IP address, and
- the public keys of the respective access means 11_1, 21_1.
10

The transaction ID from the requesting application 10_1 (via its access means 11_1), the user ID of the requesting application, and the encrypted user ID of the information providing application will be logged in the central server means 30_1.

15

In the access means 11_1 of the requesting application 10_1, the digital signature of the central server means 31_1, with its public key, is authenticated. The requesting access means 11_1 will perform a transformation of the XML node tree to an XML transport
20 file with the general XSLT file (the XSLT file for that particular DTD ID) (XSL Transformation; XSL is e.g. described in XSL Transformations (XSLT) Version 1.0, W3C Rec. dated 10 November 1999 and XSL Transformations (XSLT) Version 1.1 W3C Working draft, 12 December 2000, which documents herewith are incorporated herein
25 by reference).

The requesting application access means 11_1 optionally validates the received end user specific DTD against the XML transport file. Next the XML-file will be signed. If there is a request for
30 something, via an XML attribute, for which access is not allowed, an error message will be returned to the requesting application 10_1 by one of the access means.

If however the validation can be completed without errors, the requesting application access means 11_1 sends, to the access means 21 of the information providing application, IV,:

5
- the XML transport file (as in band information) and out of band information, e.g. in the form of a Cookie, i.e. the digital signature for the XML transport file with the private key of the access means 11_1,
- the digital signature of the out of band information from the
10   central server means 30_1, which means the server ID,
- encrypted end user ID (user ID of the information providing application),
- time to live,
- inactivity time,
15 - response time,
- the validation of the information providing side,
- DTD ID, and
- the public keys of respective access means 11_1, 21_1.

20 In one implementation, particularly discussed with reference to Fig. 5, implementing caches in association with the respective access means, a session ID of the information providing side can be included as well. If, however, there is no session, the session ID will be zero.
25

The requesting application access means 11_1 here uses HTTPS for communication with the access means of the information providing side, (IV). Next, the requesting application access means 11_1 will add the end user specific DTD into the XML transport file.
30

If the requesting application access means 11_1 does not receive any response from the access means 21_1 of the information providing application within a predetermined time interval, out of

26

band information from the central server, the requesting
application access means 11_1 will disconnect the (TCP;
Transmission Control Protocol) connection. It will also empty the
session data after a predetermined number of attempts to get a
5   response from one and the same access means on the information
providing side. Possibly it will be done after one or more
attempts on other access means of the information providing
application, in case there is for example a cluster, multiple
access means or duplicated access means or similar.
10

When the information providing application access means 21_1
receives the request, (IV), it retrieves, using the DTD ID:

- the public key of the central server,
15   - the ID of the central server and the general DTD, and,
- the general XSLT file for the particular DTD ID from its
database 22_1.

The digital signature by the requesting side access means 11_1 of
20   the XML transport file is verified against the public key of the
requesting side access means from out of band information, DTD ID,
central server ID and central server 31_1 signature of the out of
band information against the database 22_1. The XML request is
validated against the end user-specific DTD from the central
25   server 31_1. If the request is invalid, an error message is
returned to the access means 11_1. If the request is valid, the
information providing side user ID is decrypted. If the session on
the providing side is still active, or ongoing as given by the out
of band information, then there is no need for a decryption of the
30   information providing side user ID, since the session is still
alive in a decrypted form. The XML file is then parsed to an XML
node tree and, here, information providing application 20_1 is
invoked by sending the XML node tree container, a generated

transaction ID, ID of the DTD over RMI. Every new DTD ID may be validated by the information providing side access means 21_1 against the general DTD each time the server is activated. This general DTD represents the maximum data elements the information
5 providing application is prepared to release — or to have modified, in the "push" case.

For the particular session, and in communication with the information providing application 20_1, the access means 21_1 will
10 use the out of band parameter time to live (or inactivity time), V.

The information providing application 20_1 then checks what information should be get or set from the XML node tree form and
15 sends a response, VII, to the corresponding access means 21_1 containing an XML node tree filled with the requested information, and also information about completion status. The XML node tree is returned from the information providing application 20_1, after fetching information, VI, from information holder 23, back to the
20 respective access means 21_1 in an XML node tree container.

The information providing application access means 21_1 then transforms the XML node tree received from the application 20_1 to an XML transport file with the general XSLT file for that DTD ID.
25 An answer is then sent over HTTPS with the new XML transport return file to the access means 11_1 of the requesting application 10_1, VIII.

If, however, there was no response from the information providing
30 application, i.e. if the defined time period, within which a response should be provided, has lapsed, corresponding to out of band information from the central server, the access means 21_1 on the information providing side sends a reasoned notification back

28

to the access means 11_1 of the requesting side. A reasoned
notification or an error message, either from the access means on
the providing side or from the information providing application,
should be sent as out of band information back towards the access
5   means of the requesting application as a cookie with data from the
access means on the information providing side. For a successful
request, there will be no error message in the cookie.

If the requesting side access means 11_1 disconnects the TCP
10   connection to the information providing side access means 21_1, it
will have as a result that the providing side access means 21_1
disconnects the connection with the information providing
application 20_1 in a controlled manner.

15   As the access means 11_1 on the requesting side receives the XML
transport file, it parses it to an XML node tree. It returns the
XML node tree in the XML node tree container with session ID and
possible error messages, if there are any, to the requesting
application 10_1, IX. If a cache is implemented, as schematically
20   illustrated in Fig. 5, a session or object data can be stored into
said cache for a given time period, and the XML node tree
container with the session ID can be reused for the subsequent
request for the same session as long as the relevant information
is still stored in the cache.
25

As already has been indicated above, for in band information an
XML file is used between the respective access means, and DTDs are
sent from the central server means towards the respective access
means over HTTP with SSL (Socket Secure Layer).
30

For out of band information from the respective access means
towards the central server means 31_1 preferably HTTP (SSL) body is
used, and for an out of band information response from the central

server means, preferably a cookie, or some other information
field, is used.

In a particular implementation all transaction ID:s from the
5   requesting application with providing side user ID are logged in a
log file in the access means on the requesting side. Preferably
the logging can be turned on or off. Similarly all transaction
ID:s which are generated by the access means on the providing side
with encrypted user ID:s of the providing side can be logged in
10   the access means on the providing side. Preferably also this
logging is can be turned on or off.

An access means is according to the invention able to act both as
an access means for a requesting side and for an information
15   providing side, i.e. the access means are similar and provide the
relevant functionality in acting in the requesting procedures as
well as in the providing procedures.

In a particular embodiment the requested information may comprise
20   one or more binary attachments.

In one implementation an attached password may optionally be
enclosed which is used with the providing side user identification
to allow access by any user providing this password.
25

Fig. 5 illustrates an implementation with caching of sessions. The
functioning is in principle similar to that described with
reference to Fig. 4. It is illustrated how the requesting
application 10_2 communicates with the requesting side access means
30   11_2, which fetches information from, or accesses information in,
an associated database 12_2 as described above, and session
information in cache 14_2. In a similar manner, at the information
providing side, an application 20_2 communicates with access means

21_2 associated with a database 22_2 and a cache 24_2. The figure also illustrates the central server means 30_2, i.e. central server 31_2 and protection profile holding database 32_2.

5   It is here supposed that the requesting application 10_2 makes a request for a user in a non-timed out session. Steps II, III, (cf. Fig. 4) are then omitted, and the access means 21_2 of the providing side continues to request the information from the information providing application 20_2. At the requesting side, the

10   returned XML node tree container from access means 11_2 can be reused for the subsequent request for the same session. Since the XML node tree container contains a session ID, the access means 11_2 on the requesting side will reuse the same session. The returned XML node tree container advantageously also contains

15   status messages and returned XML node tree. If there are more than one access means, e.g. for reasons of redundancy, and an application wants to reuse existing session data from an earlier invocation by the application, the application generally has to access the same access means within the cluster, using the same

20   session ID as it used at the preceding invocation.

With reference to Fig. 6 an alternative implementation is illustrated in which the information providing side handles the communication, via its access means 21_3, with the central server

25   means, i.e. the central server 31_3. Such an implementation could however produce an increased load on the information providing side in case of rejected requests, as compared to the embodiments discussed above. (Also here may of course reuse of session ID be implemented.)

30

It is supposed that requesting application 10_3 makes a request for user information to its access means 11_3, I'. The access means 11_3 encrypts the user ID used by the requesting application and a

random number with the private key of the central server 31_3 to assure that it will only be understandable to the central server 31_3. Requesting side access means 11_3 then signs the user ID and the XML node tree, as discussed above with reference to Fig. 4,

5   with the private key of the access means. The request is then sent to the access means 21_3 of the providing side over Internet (or other IP-network), HTTPS, II', III'. Subsequently the request is received on the providing side access means 21_3, which signs the request and sends it to the central server 31_3, IV', for

10 decryption.

The central server 31_3 in communication with the database holding personal protection profiles 32_3, checks the signatures of the respective access means and decrypts the user ID. The providing

15 side user ID is looked up and it is established to which extent the requested access is allowable, i.e. user information can be accessed by the requesting application according to the personal protection profile of the user stored in the database. The request is updated with the access rights, e.g. request granted (e.g. to

20 limited extent) or denied etc., and the response is returned to the providing side access means 21_3, V', using HTTPS. It is here, however, supposed that the access request was granted.

The providing side access means 21_3 then sends a query, VI', to

25 the information providing application 20_3 for the information that was authorized by the central server 31_3. In communication with the database information holder, VII', the information providing application 20_3 returns the information to the access means 21_3, VIII'. The providing side access means 21_3 then returns the

30 authorized information towards the requesting side using the HTTPS session, IX', X'. The authorized information is then received by the requesting side access means 11_3, which returns the information requested by the requesting application that was

authorized, XI'. Instead of fetching information for example from
the database or information holder DB 23₃, data can also be set in
for example DB 23₃, the functioning will in principle be the same,
but information would then be provided to the "providing"
5   application instead of requested therefrom.

Fig. 7 is a somewhat generalized flow diagram describing the steps
of the procedure illustrated with reference to the block diagram
of Fig. 4. The requesting application is here denoted A1 and the
10   information providing application is denoted B1.

It is supposed that a push/pull request (i.e. a request to set or
get data) with A1 user ID, XML transport object, DTD information
etc. is sent from requesting application A1 to A1 access means,
15   100. A1 does not know who the receiver is, A1 only has knowledge
about the relevant DTD. Particularly RMI is used and the request
comprises an XML node tree transported in a container.

The access means A1 finds the address to the central server means
20   in its associated database, using the received information about
the DTD, which means that it finds the URL in the database to the
appropriate central server means. In the database all relevant
DTDs are contained. A1 access means subsequently signs in band and
out of band data, and sends it to the central server means using
25   e.g. HTTPS, 102. The central server means then finds the user ID
of the information providing application B1, encrypts the B1 user
ID, and examines if the request should be allowed using protection
profile information in the associated database, which is signed,
and subsequently digitally signs the request (if allowed), 103.
30

It is thus established if access is allowed, 104. If not, an error
message is returned to A1 access means, 105. If however access is
granted to all requested data, or to some of the requested data,

the request is returned to A1 access means which authenticates the digital signature of the central server and optionally validates the request, 106. If the optional validation, 107, is not successful, an error message is returned to application A1, 108.

5 If on the other hand, the optional validation is successful, the request is digitally signed in A1 access means and sent to application B1, using e.g. HTTPS, 109.

In B1 access means the user ID is decrypted, the digital
10 signatures of the access means A1 and of the central server means are verified, and the request is validated. The request is subsequently signed by B1 access means and a confirmation of the validation is provided to the access means A1, 110. The signed request is then forwarded from B1 access means to application B1
15 using an XML transport object over RMI, 111. Application B1 accesses the requested data and returns the requested information to B1 access means in an XML transport object, 112, (data may also be set within the requested personal profile, in an alternative implementation). (If there was no response from the information
20 holding means holding the requested personal profile data in time, an error message is instead returned.) Subsequently the B1 access means validates the XML transport file and signs the information received from application B1, 113. When application B1 accesses the requested data, it is performed e.g. by converting the request
25 to a database call and for example by checking a filled in note or form, or contacts another node/application for information.

B1 access means sends the information, after duly digitally signing it, to A1 access means using HTTPS, 114. The object has
30 then been converted to an XML transport file, and in A1 access means it is converted to an object tree, which is sent to application A1 over RMI using an XML transport object (XML node tree container), 115.

Fig. 8 is a very simplified flow diagram illustrating how a cache
can be implemented in association with the respective access means
for storing of session related information. The first step, 200,
5   corresponds to step 100 of Fig. 7. Then it is established if the
requested session and the session ID of the requested session are
stored in the cache as previously used, 201, which in practice
means that the access means of B1 has cached the encrypted user ID
of application A1. If yes, the returned XML transport object is
10   reused, in other terms, the session is reused, 202. Then it is
proceeded with step 109 of Fig. 7 cf. seq., 204. If however there
was no session stored in the cache, it is proceeded with step 101
of Fig. 7 etc., 203.

15   Fig. 9 is a flow diagram schematically illustrating an embodiment
in which the requesting application, herein denoted A2, is not
trusted, i.e. when the user ID should not be recognized by
application A2. The gateway of application A2 then uses an
encrypted user ID. In a first step, an encrypted user ID is sent
20   from the gateway to application A2, 300. Optionally the user ID
may contain a time stamp to assure that the encrypted ID is
different each time A2 is contacted by the gateway. Application A2
sends the encrypted user ID and the gateway ID to the access means
of the application A2, 301. A2 access means subsequently sends the
25   encrypted user ID and the gateway ID to the central server means,
302. The central server means selects a decryption key based on
gateway ID and decrypts the user ID, 303. It is subsequently
proceeded with steps 103 through 115 of Fig. 7, 304.

30   In Fig. 10 an alternative implementation is illustrated for a case
when the requesting application A3 is not trusted, and when the
user ID should not be recognized by A3. In this implementation the
gateway of application A3 uses a temporary user ID. Thus,

temporary user ID is sent from the gateway to application A3, 401. The gateway also sends the real user ID to an LDAP (Lightweight Directory Access Protocol) server, 402, with a possibility to map to the temporary user ID. Application A3 sends the temporary user ID and the gateway ID to A3 access means, 403, (c.f. steps 100, 101, 102 of Fig. 7). A3 access means sends the temporary user ID and the gateway ID to the central server means, 404. Thereupon the central server means invokes the LDAP database via the LDAP protocol, gets the real user ID based on gateway ID and temporarily maps the real user ID onto the temporary user ID, 405. The steps III – IX of Fig. 4 then proceed without modification, substantially corresponding to step 103 et. seq. of Fig. 7, 406. Through these implementations support is provided for not trusted applications, such as when an encrypted user ID from a WAP (Wireless Application Protocol) gateway, for mobile Internet applications, is used, or when a temporary user ID from a WAP gateway towards the application, also for mobile Internet applications, is used.

Fig. 11 illustrates a procedure when the access means are updated by the central server. It particularly relates to making changes to a DTD. It is here supposed that the central server means is updated with a new general DTD for a DTD ID, 500. The central server means updates its database holding personal protection profile data etc. Then the central server changes all end user specific DTDs for the DTD (i.e. service) with a given ID, 501. The central server pushes out the new general DTD file (signed) to all concerned access means using e.g. HTTPS, 502. The information contained in the DTD file comprises the general DTD version, DTD ID and the time when the DTD will become valid, signed with the private key of the central server means. It is then established if the pushed out files are acknowledged by access means i, 503. If yes, access means i will be registered as updated, 504. The

previous DTD version and file information are stored in access
means i, 505, to provide for backwards compatibility. Subsequently
access means i notifies the corresponding application to the
effect that it has been updated, 506.

5

It is supposed that a given number, x, of push attempts are
allowed, such that if a push j was not acknowledged for access
means i, it is examined if push attempt number j is lower than x,
507, 508. If j < x, a new push attempt is tried as from step 502

10 etc. If however j is equal to x, the access means will be updated
at a later stage, e.g. through detection via communication with
other access means or by means of a response from the central
server, 509. Then it is proceeded with step 505.

15 Registration of end users can be performed in any appropriate
manner.

Fig. 12 is a flow diagram illustrating how an end user can control
the granting/rejection of access to personal information, i.e. how

20 the end user can control which applications should be granted
access or not, and to which data etc.

In the flow diagram of Fig. 12 it is schematically illustrated one
example of end user actions that should be performed in order to

25 set a personal protection profile in order to lock and unlock
respectively personal information within the personal profiles for
different requesters. First it is supposed that the end user logs
in to the central server means when connecting to the central
server over e.g. HTTPS (it is supposed that the end user is

30 registered in the central server means), 600. Subsequently the end
user makes changes or sets up a protection profile by locking and
unlocking different data elements. This can be done in many
different ways, different protection profiles or profile levels

may be predefined, or the selection of locked and unlocked data elements etc. may be performed in a more manual way etc. taking legal requirements into account, which advantageously should be provided for automatically. The (new) "protection profile" is then 5 saved, 602. As a confirmation, and if the end user has selected an option to be notified on changes, the central server sends a notification, 603, over e.g. SMS (Short Message Service) or as an E-mail to the user. As briefly mentioned above, it is also possible to lock or unlock a complete DTD.

10

It should be clear that the invention of course not is limited to the specifically illustrated embodiments, but that it can be varied in a number of ways without departing from the scope of the appended claims.

CLAIMS

5   1. A system for end user control of the distribution and
maintenance of end user personal profile data in a data
communications system providing communication between applications
comprising and/or communicating with service/information/content
providers or holding means (DB) holding end user personal profile
10   data,
c h a r a c t e r i z e d   i n
that it comprises a personal profile protection network with at
least one central protection server means, comprising or
communicating with information holding means holding personal
15   protection profile information, and a number of distributed access
means, e.g. software modules, whereby for each of said
applications at least one access means is provided, and in that
grant/reject of an access request for/to end user personal profile
data by a requesting application is determined by the central
20   protection server in communication with a requesting application
and/or an information providing application, in that translating
means are provided for identity translation and that the identity
of a requesting application will be concealed for an information
providing application, and vice versa.
25

2. A system according to claim 1,
c h a r a c t e r i z e d   i n
that there is one access means for each application.

30   3. A system according to claim 1 or 2,
c h a r a c t e r i z e d   i n
that there are a plurality, e.g. a cluster, of access means for at
least one application.

39

4. A system according to claim 1, 2 or 3,
c h a r a c t e r i z e d   i n
that the central server means only comprises personal protection
5   profile data, the personal profile data being distributed
throughout the system.

5. A system according to claim 4,
c h a r a c t e r i z e d   i n
10 that the personal protection profile data comprises information
about, for each end user of the system, which of the end user
personal profile data that should be accessible by which
application(s).

15 6. A system according to claim 4,
c h a r a c t e r i z e d   i n
that the personal protection profiles are assigned one of a given
number of security levels, the lowest level e.g. indicating that
for all personal profile data access is prevented for every
20 application, the highest e.g. indicating that all personal profile
data is freely available.

7. A system according to any one of the preceding claims,
c h a r a c t e r i z e d   i n
25 that the interface between an application and the respective
access means comprises an Application Programmable Interface (API)
based on (using) a generic markup language.

8. A system according to claim 7,
30 c h a r a c t e r i z e d   i n
that the generic markup language is XML.

9. A system according to claim 7 or 8,

40

c h a r a c t e r i z e d   i n

that access to requested end user personal profile data is granted/rejected by the central server in communication with the requesting application.

10. A system according to claim 7 or 8,

c h a r a c t e r i z e d   i n

that access to requested end user personal profile data is granted/rejected by the central server in communication with the information providing application.

11. A system according to claim 7 or 8,

c h a r a c t e r i z e d   i n

that access to requested end user personal profile data is granted/rejected by the central server in communication with the requesting application and the information providing application.

12. A system according to claim 9, 10 or 11,

c h a r a c t e r i z e d   i n

that first user identity translating means (e.g. encrypting means) are provided at least in the central server means.

13. A system according to claim 10, 11 or 12,

c h a r a c t e r i z e d   i n

that second user identity translating means are provided in the access means of the requesting application.

14. A system according to any one of claims 7-13,

c h a r a c t e r i z e d   i n

that for an application being part of the system a general DTD (Document Type Definition) is given to define maximum allowed flow of personal data.

41

15. A system according to claim 14,
c h a r a c t e r i z e d   i n
that for each user a specific user DTD is given to define allowed
flow of personal data for this particular user.

5

16. A system according to any one claims 7-15,
c h a r a c t e r i z e d   i n
that an access request for end user profile data is transported
from the requesting application to its access means e.g. using
10   RMI, and in that the access request includes a user identity
associated with the requested personal end user profile.

17. A system according to claim 16,
c h a r a c t e r i z e d   i n
15   that the request is transported as an XML transport object (XML
Node tree container) tagged with information about the requested
end user personal profile data.

18. A system according to claim 16 or 17,
20   c h a r a c t e r i z e d   i n
that the HTTPS protocol is used for communication between the
access means of the requesting/information holding application and
the central server means.

25   19. A system according to any one of the preceding claims,
c h a r a c t e r i z e d   i n
that the access means of the information requesting and/or
providing application(s) comprise(s) means for encrypting the user
identity associated with the requested end user profile.
30

20. A system according to any one of the preceding claims,
c h a r a c t e r i z e d   i n

42

that the request is digitally signed with a private key of the
access means of the requesting application and/or with a private
key of the access means of the information providing application.

5   21. A system according to claim 20,
c h a r a c t e r i z e d   i n
that the request is digitally signed with a private key of the
central server means, and in that the digital signature(s) of the
access means are verified in the central server means.
10

22. A system according to claim 21,
c h a r a c t e r i z e d   i n
that the central server means comprises means for encrypting at
least the user identity associated with the requested information
15   used by the information providing information.

23. A system according to any one of the preceding claims,
c h a r a c t e r i z e d   i n
that at least some of the applications comprise a cache memory
20   respectively for temporarily holding information about access
requests, such that a previously used session can be reused, at
least for a given time period.

24. A personal profile (privacy) control network for controlling
25   the access to personal profile data,
c h a r a c t e r i z e d   i n
that it comprises at least one central protection server means,
comprising or communicating with information holding means holding
personal protection profile information, and a number of
30   distributed access means, e.g. software modules, at least one
access means respectively interfacing each of a number of
applications, the central protection server means comprising means
for translating and verifying identities, and in that a request

43

for access to personal profile data by a requesting application is
communicated to the requesting application access means and
granted/rejected by the central server means in communication with
the access means of the requesting application and/or the
5   information providing application, and in that the user identity
used by the requesting application is concealed for the
information providing application and vice versa.

25. A personal profile control network according to claim 24,
10   c h a r a c t e r i z e d   i n
that the interface between an application and the respective
access means is based on a generic mark-up language.

26. A personal profile control network according to claim 25,
15   c h a r a c t e r i z e d   i n
that the generic mark-up language is XML.

27. A personal profile control network according to any one of
claims 24-26, c h a r a c t e r i z e d   i n
20   that the information holding means of the central server means
comprises, for each user of the system, a personal protection
profile, and in that the personal protection profiles are end user
controlled.

25   28. A personal profile control network according to claim 27,
c h a r a c t e r i z e d   i n
that the central server means and at least one of the information
requesting/providing access means digitally sign a request for
personal profile data with the respective private key, and in that
30   the digital signatures are verified by the central server means.

29. A method of controlling access to personal data within a
personal end user profile in a data communication network running

a number of applications comprising or communicating with
information holding means,
c h a r a c t e r i z e d   i n
that it comprises the steps of:

5   - providing an access request from a requesting application to an
       access means associated with the requesting application using a
       generic mark-up language, e.g. XML,

     - forwarding the request from the access means to a central
       server means with information holding means holding personal
10   protection profiles for the end users in the system;

     - performing user identification encryption, such that the user
       identification of the requesting application will be concealed
       from an information providing application, and vice versa;

     - establishing, by using the request and the personal protection
15   profile whether access is to be granted or denied;
       if access to the requested personal profile is to be granted,

     - confirming to the access means of the requesting application
       whether access is to be granted or not, preferably after
       digitally signing the request;

20   - allowing transfer of the encrypted and preferably digitally
       signed request to the information providing application.

     30. The method according to claim 29,
     c h a r a c t e r i z e d   i n
25   that the request of a requesting application relates to getting
     access to data/fetching data in a personal profile and in that,
     for a granted request, the method comprises the step of:

     - transferring the requested data via the access means of an
       information providing application over a data communication
30   network, e.g. Internet, to the access means of the requesting
       application.

     31. The method according to claim 29,

45

c h a r a c t e r i z e d   i n

that the request of a requesting application relates to setting/
updating data in a personal profile, and in that, for a granted
request the method further comprises the step of:

5   - transferring the data to be set/updated data to the information
providing application over the data communication network.

32. A method of controlling access to personal data within a
personal end user profile in a data communication network running
10   a number of applications comprising, or communicating, with
information holding means,

c h a r a c t e r i z e d   i n

that it comprises the steps of:

- forwarding a request for access to data within a personal
15   profile from a requesting application via at least one
distributed access means to a central server means;

- establishing in the central server means whether access to
requested data should be allowed or not by comparing the
request with an end user controlled personal protection
20   profile;

- providing the at least one distributed access means with
information as to whether access is allowable or not, such that
if access is allowable, the data communication network can be
used for giving the requesting application access to the
25   requested data without the identity of the requesting
application being visible to the application able to provide
access to the requested data, and vice versa.

33. A method according to claim 32,
30   c h a r a c t e r i z e d   i n

that it further comprises the steps of:

46

- encrypting a user identity associated with the requested end
  user profile into the request at the central server means or at
  access means associated with the requesting application;
- decrypting the user identity at access means associated with
5   the information providing application.

34. The method according to claim 32 or 33,
c h a r a c t e r i z e d   i n
that it comprises the steps of:
10 - digitally signing the request at one or more of the access
      means associated with the information requesting application,
      the access means associated with the information providing
      application and the central server means, said access means and
      the central server means constituting a personal profile data
15   protection network.

1/11

STATE OF THE ART

Fig. 1

Fig.2

Fig. 3

4/11

Fig. 4

Fig.5

Fig.6

PUSH/PULL REQ. WITH APPL. A1 USER ID., XML TRANSPORT ── 100
OBJ., DTD (SERVICE) INFO FROM APPL A1 TO A1 ACCESS MEANS

A1 ACESS MEANS FINDS ADDRESS TO CENTRAL SERVER MEANS ── 101
IN ITS DB USING RECEIVED DTD (SERVICE) INFO

REQUEST FROM A1 ACCESS MEANS TO CENTRAL ── 102
SERVER MEANS USING HTTPS

CENTRAL SERVER MEANS ENCRYPTS USER ID. OF INFO
PROVIDING APPL. B1 AND ESTABLISHES IF REQUEST ── 103
ALLOWABLE USING PROTECTION PROFILE INFO IN
ASSOCIATED DB AND DIGITALLY SIGNS REQUEST

104 — ACCESS   NO   ERROR MSG AND XML TRANSPORT OBJ. ── 105
ALLOWED   RETURNED TO A1 ACCESS MEANS
?

YES   ── 106

REQUEST RETURNED TO A1 ACCESS MEANS WHICH AUTHENTICATES DIGITAL
SIGNATURE OF CENTRAL SERVER AND OPTIONALLY VALIDATES REQ.

107 — OPTIONAL   NO   ERROR MSG RETURNED ── 108
VALIDATION   TO APPL A
O.K. ?

YES

REQUEST DIGITALLY SIGNED IN A1 ACCESS MEANS ── 109
AND SENT TO APPL. B1 USING HTTPS

B1 ACCESS MEANS VERIFIES SIGNATURES, DECRYPTS USER ID,
VALIDATES REQUEST. REQUEST SIGNED BY B1 ACCESS MEANS, ── 110
VALIDATION CONFIRMED TO A1 ACCESS MEANS

REQ. FROM B1 ACCESS MEANS TO APPL. B1 USING XML TRANSPORT OBJ. ── 111

APPL. B1 ACCESSES REQ. DATA AND RETURNS INFO ── 112
TO B1 ACCESS MEANS IN XML TRANSPORT OJECT

B1 ACCESS MEANS VALIDATES AND SIGNS RECEIVED INFO ── 113

INFO TO A1 ACCESS MEANS USING HTTPS ── 114

INFO TO APPL. A1 USING XML TRANSPORT OBJECT ── 115

Fig. 7

8/11

```
200 ──┐ ┌─────────────────┐
       │ CF STEP 109 ET SEQ.│
       │ OF FIG. 7          │
       └─────────────────┘
```

                                                    ┌── 202
                                          ┌──────────────────────┐
201 ──┐   ◇ REQUESTED   YES   │ REUSE RETURNED XML   │
       │   SESSION STORED   ─────────────│ TRANSPORT OBJECT, I.E │
           IN CACHE UNDER SESSION ID.   │ REUSE SESSION   │
            AS PREVIOUSLY USED   └──────────────────────┘
                  ?
                 │ NO   ┌── 204
                 ▼   ┌─────────────────┐
203 ──┐ ┌─────────────────┐   │ STEP 109 OF FIG. 7│
       │ STEP 101 OF FIG. 7│   │ ET. SEQ.   │
       │ ET. SEQ.   │   └─────────────────┘
       └─────────────────┘

Fig.8

       ┌────────────────────────┐
       │ ENCRYPTED USER ID. FROM │───── 300
       │ GATEWAY TO APPL. A2   │
       └────────────────────────┘
                 │
                 ▼
       ┌──────────────────────────────┐
       │ APPL. 2 SENDS ENCRYPTED USER ID. AND │───── 301
       │ GATEWAY ID. TO B2 ACCESS MEANS │
       └──────────────────────────────┘
                 │
                 ▼
       ┌──────────────────────────────┐
       │ B2 ACCESS MEANS SENDS ENCRYPTED│
       │ USER ID. AND GATEWAY ID TO   │───── 302
       │ CENTRAL SERVER MEANS   │
       └──────────────────────────────┘
                 │
                 ▼
       ┌──────────────────────────────┐
       │ CENTRAL SERVER MEANS SELECTS DECRYPTION│
       │ KEY BASED ON GATEWAY ID. AND DECRYPTS │───── 303
       │ USER ID.   │
       └──────────────────────────────┘
                 │
                 ▼
       ┌─────────────────┐
       │ STEP 103 ET SEQ │───── 304
       │ OF FIG. 7   │
       └─────────────────┘

Fig.9
```

```
┌─────────────────────────────┐
│ TEMPORARY USER ID. FROM     │──── 401
│ GATEWAY TO APPL. A3         │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│ REAL USER ID. FROM GATEWAY TO │──── 402
│ AN LDAP SERVER              │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│ APPL. A3 SENDS TEMPORARY USER ID. AND │──── 403
│ GATEWAY ID. TO A3 ACCESS MEANS │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│ A3 ACCESS MEANS SENDS TEMPORARY │──── 404
│ USER ID. AND GATEWAY ID. TO CENTRAL │
│ SERVER MEANS                │
└─────────────────────────────┘
              │
              ▼
┌─────────────────────────────┐
│ CENTRAL SERVER MEANS INVOKES LDAP DB VIA │──── 405
│ LDAP PROTOCOL, GETS REAL USER ID. BASED │
│ ON GATEWAY ID. AND TEMPORARILY MAPS │
│ REAL USER ID. AGAINST TEMPORARY USER ID. │
└─────────────────────────────┘
              │
              ▼
       ┌──────────────┐
       │ STEP 103 ET  │──── 406
       │ SEQ. OF FIG 7 │
       └──────────────┘
```

Fig. 10

CENTRAL SERVER MEANS UPDATED WITH A NEW GENERAL DTD FOR A SPECIFIC SERVICE —500

CENTRAL SERVER CHANGES ALL END USER INSTANTIATED DTD:S FOR A SPECIFIC SERVICE —501

CENTRAL SERVER PUSHES OUT NEW GENERAL DTD FILE TO ALL CONCERNED ACCESS MEANS USING E.G. HTTPS —502

503 — PUSHED-OUT FILE ACKNOWLEDGED BY ACCESS MEANS i ?

NO → PUSH ATTEMPT j COUNTED —507

j < x ? —508

NO

YES

ACCESS MEANS i REGISTERED AS UPDATED —504

YES

ACCESS MEANS i UPDATED AT LATER STAGE E.G. THROUGH DETECT. VIA OTHER ACCESS MEANS OR RESPONSE FROM CENTRAL SERVER

PREVIOUS DTD AGREEMENT VERSION AND FILE INFO STORED IN ACCESS MEANS i —505

ACCESS MEANS NOTIFIES APPLICATION

506

509

Fig. 11

 END USER LOGS IN TO CENTRAL SERVER
MEANS OVER E.G. HTTPS OR WAP ———— 600

END USER SELECTS DTD, LOCKS/ UNLOCKS
DIFFERENT DATA ELEMENTS ACC. TO ———— 601
PERSONAL PROTECTION PROFILE

CHANGES SAVED ———— 602

NOTIFICATION ABOUT PERFORMED
CHANGES SENT FROM CENTRAL ———— 603
SERVER MEANS TO END USER

Fig. 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/01832

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 17/60, G06F 17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0150299 A2 (PANGO SYSTEMS B.V.), 12 July 2001 (12.07.01), page 14, line 28 - page 16, line 22 --	1-34
A	EP 0991005 A2 (NCR INTERNATIONAL INC), 5 April 2000 (05.04.00), paragraphs 9-16 --	1-34
A	US 6285983 B1 (JENKINS, E.D.), 4 Sept 2001 (04.09.01), column 2, line 31 - column 4, line 10 -- --------	1-34

☐ Further documents are listed in the continuation of Box C.   ☒ See patent family annex.

*	Special categories of cited documents:
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier application or patent but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed

"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 January 2003	29 -01- 2003

Name and mailing address of the ISA/	Authorized officer
Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Anders Edlund/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE 02/01832

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
WO	0150299	A2	12/07/01	AU	1882501	A	16/07/01
EP	0991005	A2	05/04/00	JP	2000293421	A	20/10/00
				US	6253203	B	26/06/01
				US	6480850	B	12/11/02
US	6285983	B1	04/09/01	AU	1215800	A	08/05/00
				EP	1131763	A	12/09/01
				WO	0023932	A	27/04/00

Form PCT/ISA/210 (patent family annex) (July 1998)